Security Architecture Work Group
Disaster Recovery and Business Continuity

Tuesday June 11, 2002
1:30 P.M. to 3:00 P.M.
NSOB LLF -- Lincoln

Minutes

A. Participants

Brett	Anderson	Military Department
Cathy	Danahy	Secretary of State / Records Management
Dwayne	Dvorak	University of Nebraska
Scott	Evers	Dept of Labor
Jerry	Hielen	IMServices
Joe	Kellner	Department of Roads
Steve	Schafer	Nebraska CIO
Ron	Schrock	Military Department
Ron	Woerner	Department of Roads

B. General Discussion

Discussion covered the importance of developing a sound business case and the need for enforcement. For example, the Military Department cannot connect to the Department of Defense network, unless they meet certain accreditation standards that include a business continuity plan. The importance of telecommunications to disaster recovery was also discussed.

Cathy Danahy gave an overview of the activities of the Records Management Division that relate to disaster recovery. They are responsible for implementing the Records Management Act, which applies to all state agencies and local governments. Compliance requires every entity to prepare a records retention schedule. The Records Management Division has dealt with some aspects of disaster recovery. In the past they have focused on the physical aspect of cleaning and restoring paper records that are damaged in a disaster. The division serves as a repository for back-up media for many state agencies. Some of these are active records. They are looking at a contract with a company that would help to restore records, if they are damaged. The company provides planning assistance at no cost. The Records Management Division might be able to serve as a repository of agency disaster recovery plans.

Participants listed some of their goals for a work group on business continuity. These included:

- Developing definitions and a division of that distinguish between IT-related disaster recovery and the broader concept of business continuity;
- Preparing a handbook that agencies can use, which retains flexibility for meeting individual needs of agencies;
- Identify opportunities for cooperation among agencies;
- Share ideas;
- Address the need for testing of disaster recovery and business continuity plans;
- Provide guidance in identifying critical systems and critical business functions;
- Encourage partnerships between entities, using the military's inter-service agreements as a model;

- Address “out-of-scope” issues by making recommendations to other entities that have those responsibilities (finding space for alternative sites is an example);

Participants discussed the need for other agencies to be actively involved in disaster recovery for IT. Examples included the Division of Communications (telecommunications services), Department of Revenue, and local government.

C. Next Steps

Participants identified the following steps to guide work on disaster recovery and business continuity:

1. Prepare a statement that describes the scope, underlying assumptions, and relationship of this effort to business continuity and NEMA’s State Emergency Operations Plan. (Steve Schafer will prepare a draft statement for consideration at the next meeting.)
2. Endorse using the “Contingency Planning Guide for Information Technology Systems” published by the National Institute of Standards and Technology (NIST) in June 2002 as the basis for the state’s guidelines. The document is posted at http://csrc.nist.gov/publications/nistpubs/index.html. (Any concerns or caveats about using this document should be brought to the next meeting.)
3. Define the overall process for disaster recovery planning and contingency planning. Page 14 of the NIST guide identifies seven key elements:
    a. Develop the contingency planning policy statement
    b. Conduct the business impact analysis (BIA)
    c. Identify preventive controls
    d. Develop recovery strategies
    e. Develop an IT contingency plan
    f. Plan testing, training, and exercises
    g. Plan maintenance.
4. Develop a template and checklist that provides easy to follow steps. (Ron Woerner will prepare a first draft for discussion at the next meeting.)
5. Prepare a business case. The agenda for the next meeting will include a white board exercise for preparing a business case.
6. Prepare recommendations, including critical issues, opportunities for cooperation, and steps for implementation.

D. Next Meeting Date

The work group will meet again on Tuesday, July 9, 2002, from 1:30 to 4:30 (NSOB LLB). The agenda will include

1. Review statement of scope and assumptions;
2. Confirm or modify decision regarding NIST’s Contingency Planning Guide for Information Technology Systems;
3. Confirm overall process;
4. Review draft template / checklist;
5. Discuss business case;
6. Discuss recommendations.